DOE CIO Guidance CS-20

U.S. Department of Energy

Cyber Security Program

INFORMATION CONDITION (INFOCON)

GUIDANCE

October 2006

This Guidance document was developed and issued outside of the Departmental Directives Program.

1. PURPOSE.

The Department of Energy (DOE) Information Condition (INFOCON) process is a structured, coordinated approach to react to adversarial attacks on DOE information, computer systems, and telecommunication networks and systems. The intent of the INFOCON is to determine, assess, and communicate information regarding the risk of cyber attacks and define organizational defensive responses to reduce vulnerability, increase response capability, and mitigate sustained damage to DOE information and infrastructure. Every Departmental organization is impacted when the level of attack increases against any other part of the Department. The tiered approach presented in this Guidance allows a consistent set of actions to be followed locally, organizationally, or Departmentally once the need to react to attack is identified.

The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. CANCELLATIONS.

None.

3. APPLICABILITY.

a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to which DOE CIO Guidance CS-20 is Applicable*.

Further, Senior DOE Management may also specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units and for ensuring that those requirements are incorporated into contracts.

b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE guidance for activities under the NNSA Administrator’s cognizance.

c. Unclassified Systems. Senior DOE Management Program Cyber Security Plans (PCSPs) must address this Guidance for all systems hosting unclassified information. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.

d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

4. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its effective date. If Senior DOE Management cannot address all of the criteria by the scheduled milestone, Senior DOE Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

5. DOE INFOCON.

The INFOCON is a comprehensive defense posture and response based on the status of information systems, operations, and intelligence assessments of adversary capabilities and intent. It is based on a structure of graduated threat conditions that increase as the risk and threat increase and presents a structured, coordinated approach to defend against and react to adversarial attacks on operating units' information, computer systems, and telecommunication networks and systems. At each level, corresponding protective measures are initiated to reduce vulnerability or increase response capability during a period of heightened alert.

a. INFOCON Levels. Each of the following five INFOCON levels reflects a defensive posture focused on computer network-based protective responses and actions specific to the unique nature of a Computer Network Attack (CNA) and Computer Network Exploitation (CNE). The higher the INFOCON, the greater the risk of an attack. Risk includes both the probability of an attack occurring and its potential impacts.

(1) Normal (Green) Condition.

(2) Guarded (Blue) Condition.

(3) Elevated (Yellow) Condition.

(4) Severe (Orange) Condition.

(5) Critical (Red) Condition.

Table 1 shows the five INFOCON levels and corresponding recommended actions. There are three broad categories of factors that influence the INFOCON: operational, technical, and intelligence, including foreign intelligence and law enforcement intelligence. The INFOCON level is based on significant changes in one or more of them.

b. CNA/CNE Assumptions.

(1) Shared Risk. Risk assumed by one Senior DOE Management operating unit is risk shared by all. In a declared DOE INFOCON state, actions must be carried out concurrently at all locations for an effective defense.

(2) Advance Preparation. Protective measures must be planned, prepared, exercised, and often executed well in advance of an attack. Preventive measures are emphasized in INFOCON responses because there may be little time to react effectively during the attack.

(3) Anonymity of Attacker. Knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics.

(4) Characterization of the Attack. Malicious intent is assumed until an event is assessed otherwise.

c. INFOCON Assignment.

(1) OCIO

(a) INFOCONs are assigned for the Department by the OCIO. In addition, the OCIO is responsible for directing changes and developing Departmental INFOCON procedures, levels, and measures and directing and executing Department-wide INFOCON activities. The OCIO may recommend localized or organizational INFOCON changes to appropriate Senior DOE Management in lieu of changing the Departmental INFOCON.

(b) The presumed Departmental functional INFOCON level, unless otherwise determined by the OCIO, is Green (Normal).

(c) The Departmental INFOCON level is determined by the DOE OCIO and will be posted, and updated as needed, on the DOE OCIO web site. (http://cio.energy.gov/cybersecurity.htm)

(d) When the DOE INFOCON level is issued or changed, the OCIO will notify Senior DOE Management Cyber Security Working Group representative via the most rapid means available.

(e) The Departmental and Senior DOE Management INFOCON levels will be reviewed at regular intervals to determine whether adjustments are warranted based on the overall operational and security context at that time.

(2) Senior DOE Management

(a) Senior DOE Management and their operating units are responsible for implementing the INFOCON system, developing supplemental INFOCON procedures specific to their mission(s), and reporting INFOCON actions in accordance with OCIO guidance.

(b) If conditions warrant within a Senior DOE Management organization or one or more of its operating units, INFOCONs can be assigned by cognizant Senior DOE Management for all or part of its organization.

i. In such cases, Senior DOE Management is to assess the situation and establish the proper INFOCON level for the organization based on all relevant factors. Localized or organizational INFOCON levels, however, must remain at least as high as the current INFOCON directed by the DOE OCIO.

ii. Senior DOE Management is to consider the impact of localized or organizational INFOCONs on connectivity with computer networks and systems of other Departmental operating units and operations.

iii. Senior DOE Management is to notify the DOE OCIO Incident Management Division Director of increases in INFOCON levels above those directed by the OCIO.

(3) <u>INFOCON Notification</u>. INFOCON Notification will include the following information.

(a) Date/time of report.

(b) Declared INFOCON.

(c) Reason for declaration of this INFOCON, to include a detailed description of the causal activities to include Type and System Impact Category.

(d) Current/planned operation(s) or capabilities, units/organizations, networks, systems, applications or data assessed to be impacted or at risk.

(e) Any additional recommended or directed actions.

(f) References to relevant technical advisories, intelligence assessments, etc.

(g) Contact information.

(h) Information that may assist in operating unit response.

Table 1. INFOCON Levels

INFOCON LABEL	CRITERIA	RECOMMENDED ACTIONS
Normal (GREEN)	• Normal operations. • Network penetration or denial of service attempted with no impact to NNSA, DOE, or site operations such as Type 2 reconnaissance activity or intrusion attempts with a low impact. • Minimal attack success, successfully counteracted such as a Type 1 unauthorized use with a low impact. • Information system probes; scans or other activities detected indicating a pattern of surveillance such as Type 2 reconnaissance activity with a low impact. • General threat unpredictable.	• Ensure all mission critical information and information systems (including applications and databases) are identified. • Ensure personnel receive training on the INFOCON levels and specific preplanned Senior DOE Management Protective Measures. • Ensure all points of access are identified, operationally necessary, and protected with Boundary Protection Services (BPS). • On a continuing basis, conduct normal cyber security practices. • Refine and exercise preplanned protective measures. • Periodically review and test higher INFOCON actions.

INFOCON LABEL	CRITERIA	RECOMMENDED ACTIONS
Guarded (BLUE)	• Indications and warnings (I&W) indicate general threat. • Regional events occur which affect US interests, are likely to affect one or more Senior DOE Management interests, and involve potential adversaries with suspected or known CNA capability. • Information system probes; scans or other activities detected indicating a pattern of surveillance such as Type 2 reconnaissance activity with a moderate or high impact. • Network penetration or denial of service attempted with no impact to Senior DOE Management operations such as Type 2 attempted intrusion with a low impact. • Increased and / or more predictable threat events. • Nation- or Internet-wide computer network exploit such as a Type 1 web site defacement, malicious code, or denial of service with an impact of low. • CNA incident occurs at DOE or Senior DOE Management operating unit	Accomplish all actions at INFOCON Green, plus the following: • Execute appropriate cyber security practices to include closer monitoring of access points. • Heighten user awareness. • Execute appropriate defensive actions. • Follow Senior DOE Management reporting procedures. • Consider proactive execution of some, or all, higher INFOCON actions. • Review and update, as necessary, emergency response procedures.

INFOCON LABEL	CRITERIA	RECOMMENDED ACTIONS
Elevated (YELLOW)	• I&W indicate targeting of a specific system, location, unit or operation. • Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance. • Incident occurs at Senior DOE Management operating unit that affects a DOE enterprise system or may impact other Senior DOE Management operating unit such as a Type 1 compromise/ intrusion with a low impact. • Intelligence indicates imminent attack against Senior DOE Management operating unit.	Accomplish all actions at INFOCON Blue, plus the following: • Execute, as appropriate, the following cyber security practices: • Enhance review of tools looking for anomalous behavior. • Increase frequency and strengthened reviews of auditing on critical systems. • Immediately review systems for security weaknesses and patch all critical systems, as needed. • Isolate compromised systems immediately. • Report suspected incursion or incidents early following Senior DOE Management reporting procedures. • Assess planned responses in light of the precise characteristics of the threat as seen and refine planned responses, as necessary. • Check communications with designated emergency response or command locations. • Review higher INFOCON level actions. • Consider proactive execution of some or all higher INFOCON level actions.

INFOCON LABEL	CRITERIA	RECOMMENDED ACTIONS
Severe (ORANGE)	• Information system attack(s) detected with limited impact to DOE or Senior DOE Management operations. • Operating unit able to accomplish mission. • CNE at a DOE or Senior DOE Management operating unit such as Type 1 compromise/intrusion with low impact. • Nation- or Internet-wide CNE. • Intelligence indicates imminent attack against national infrastructure or national security element. • Intelligence attack assessment(s) indicate a limited attack.	Accomplish all actions at INFOCON Yellow, plus the following: • Execute, as appropriate, the following cyber security practices: • Increase frequency and strengthened reviews of auditing on critical systems. • Reconfigure Boundary Protection Systems (BPS), e.g., firewalls, routers, and intrusion prevention systems, to limit external connections and traffic to absolute minimum needed for current mission operations. • Reconfigure systems to minimize access points and increase security. • Minimize traffic among enclaves to absolute minimum needed for current mission operations. • Consider eliminating Internet access to/from all non-mission-critical systems and networks. • Isolate any compromised systems immediately. • Follow Senior DOE Management reporting procedures. • Review higher INFOCON actions. • Consider proactive execution of some, or all, higher INFOCON actions.
Critical (RED)	• Pattern of successful information system attack(s) detected which impact DOE or Senior DOE Management operations such as a Type 1 compromise/intrusion or denial of service with a moderate or high impact. • Widespread incidents that undermine ability to function effectively. • Significant risk of mission failure. • CNA against national infrastructure or national security element.	Accomplish all actions at INFOCON Orange, plus the following: • Execute, as appropriate, the following cyber security practices: • Reconfigure information systems and networks to use BPS controlled connections and traffic. • Execute procedures for ensuring graceful degradation of information systems and network(s). • Disconnect all non-mission-critical systems and networks from Internet. • Implement procedure for 'stand-alone" or manual operations. • Follow Senior DOE Management reporting procedures. • Execute applicable portions of Continuity of Operations plans.

6. CRITERIA.

   a. Program Cyber Security Plans. Senior DOE Management PCSPs are to address the following INFOCON activities.

      (1) Detail processes for rapid dissemination of INFOCON information within the Senior DOE Management organization.

      (2) Define, document, and test procedures for reporting INFOCON actions within the Senior DOE Management organization and to the OCIO.

         (a) The DOE OCIO Incident Management Division Director is to be notified, through the Senior DOE Management Cyber Security Working Group representative, of the status of actions within two (2) working hours of the issuance or change in Departmental INFOCON level.

         (b) The DOE OCIO Incident Management Division Director is to be notified, through the Senior DOE Management Cyber Security Working Group representative, within two (2) working hours of receipt of a Departmental INFOCON declaration if response measures conflict with organization or mission priorities.

         (c) Reporting to the OCIO is to include status of actions taken in response to INFOCON issuance or change within the Department, the Senior DOE Management organization, or the operating unit.

      (3) Define, document, and test procedures for changing and reporting the Senior DOE Management or operating unit INFOCON level.

         (a) Senior DOE Management or operating unit INFOCON level must be at least as high as the DOE OCIO declared INFOCON Level.

         (b) Changes in Senior DOE Management or operating unit INFOCON level are to be reported to the DOE OCIO Incident Management Division Director within two (2) working hours. The report is to contain the name of the organization, its location, date/time of report, INFOCON level, reason for declaration of this INFOCON, response actions taken, description of operational impact, Point of Contact (POC) name, and contact information. Law Enforcement Agency (LEA) case numbers should be included if they are involved.

      (4) Test INFOCON procedures annually and document operational impact assessments.

      (5) Define and document the Senior DOE Management organization's defensive posture for each INFOCON level. The factors used to determine defensive posture include the following:

(a) DOE Threat Statement and Risk Assessment

(b) Other indications & warnings (including domestic threats): National Security Agency (NSA) Alerts; National Infrastructure Protection Center (NIPC) advisories, US-CERT advisories, threats, warnings; law enforcement agency intrusion reports, etc.

(c) CNA/CNE intelligence assessments

(d) Current world situation

(e) Other alert systems such as Security Condition (SECON), etc.

(f) System criticality and readiness

(g) Status of coordination for the protection of Critical Infrastructure and Key Resources identified under Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*

(h) Incident reports

(i) Trend analyses

(j) Technical impact assessment

(k) Operational impact assessment

(l) Assessment of the potential for an information attack

(6) Require operating units to define, document, and test INFOCON response measures.

(a) Integrate response measures with local SECON procedures, emergency procedures, Continuity of Operations plans, and incident handling processes.

(b) Coordinate INFOCON events and disseminate INFOCON information in accordance with PCSP requirements.

(c) Define processes for evaluating local CNA/CNE situations and changing the local INFOCON level.

i. The INFOCON must remain at least as high as the current INFOCON directed by DOE OCIO for the Department or the Senior DOE Management for the organization.

ii. Operating unit changes in the INFOCON of a Senior DOE Management operating unit must be monitored and reported as outlined in the Senior DOE Management PCSP.

7. REFERENCES.

References are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

8. DEFINITIONS.

Definitions specific to this Guidance are defined in Attachment 2. Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

9. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-20 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2

DEFINITIONS

Access—Opportunity to make use of an information system (IS) resource.

Computer Network Attack (CNA) —Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves

Computer Network Exploitation (CNE)—Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations.

Event—Occurrence, not yet assessed, that might effect the performance of an IS.

High Impact—Loss of system confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on DOE and/or Senior DOE Management operations, assets, or individuals. The incident could cause the loss of mission capability for a period that poses a threat to human life or results in the loss of major assets.

Intrusion—Unauthorized act of bypassing the security mechanism of a system.

Low Impact—Loss of system confidentiality, integrity, and availability could be expected to have a limited adverse effect on DOE and/or Senior DOE Management operations, assets, or individuals, requiring minor corrective actions or repairs.

Moderate Impact—Loss of system confidentiality, integrity, and availability could be expected to have a serious adverse effect on DOE and/or Senior DOE Management operations, assets, or individuals, including significant degradation or major damage, requiring extensive corrective actions or repairs.

Restoration—Action taken to repair and return to service, an impaired (degraded) or unserviceable telecommunications service or facility. **Note:** Permanent or temporary restoration may be accomplished by various means, such as patching, rerouting, substitution of component parts, etc.

Type 1 incidents—Successful incidents that potentially create serious breaches of DOE and/or Senior DOE Management cyber security or have the potential to generate negative media interest.

Type 2 incidents—Incidents that pose potential long-term threats to DOE and/or Senior DOE Management cyber security interests or that may degrade the overall effectiveness of the Department's cyber security posture.